UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/632,156	07/31/2003	Ronald P. Doyle	RSW920030063US1	1905

7590 01/08/2007

Jeanine S. Ray-Yarletts
IBM Corporation
T81/503
PO Box 12195
Research Triangle Park, NC 27709

EXAMINER	
WYSZYNSKI, AUBREY H	
ART UNIT	**PAPER NUMBER**
2134	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/08/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/632,156	DOYLE ET AL.	
	Examiner	Art Unit	
	Aubrey H. Wyszynski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 July 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *See Office Action*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-32 are pending.

Information Disclosure Statement

2. The information disclosure statements (IDS) submitted on 7/18/05, 2/27/04, 11/17/03, 7/31/03 are being considered by the examiner.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-32 are rejected under 35 U.S.C. 102(b) as being anticipated by Yamada et al, U.S. Patent No. 6,144,743.

Regarding claim 1, Yamada discloses a security container/recording unit (HDD) (fig. 1, #29 and fig. 2, #29), that secures a document component by encapsulating, within the security container, the document component/encrypted information (fig. 2, #40), conditional logic for controlling operations on the document component/control information (fig. 2, #42), and key distribution information usable for controlling access to the document component/encrypted key information (fig. 2, #41).

Regarding claim 2, Yamada discloses the security container according to claim 1, wherein the security container secures a portion of a higher-level document (col. 7, lines 40-45).

Regarding claim 3, Yamada discloses the security container according to claim 2, wherein the higher-level document has more than one portion secured by security containers (fig. 10).

Regarding claim 4, Yamada discloses a method of securing document content using security containers/recording unit (HDD) (fig. 1, #29 and fig. 2, #29), comprising the step of encapsulating, within a security container, a document component/encrypted information (fig. 2, #40), conditional logic for controlling operations on the document component/control information (fig. 2, #42), and key distribution information usable for controlling access to the document component/encrypted key information (fig. 2, #41).

Regarding claim 5, Yamada discloses the method according to claim 4, wherein the key distribution information further comprises an identification of one or more users and/or processes that are authorized to access the document component/user specifying information (fig. 3, #53).

Regarding claim 6, Yamada discloses the method according to claim 5, wherein the key distribution information further comprises a symmetric key that encrypted both the

document component and the conditional logic that are encapsulated within the security container, wherein the symmetric key is stored in an encrypted form for decryption by the authorized users and/or processes (col. 9, lines 10-17).

Regarding claim 7, Yamada discloses the method according to claim 6, wherein the encrypted form of the symmetric key comprises a separate version of the key for each distinct user, process, group of users, or group of processes, wherein the separate version has been encrypted with a public key associated with the corresponding distinct user, process, group of users, or group of processes (col. 16, lines 25-34).

Regarding claim 8, Yamada discloses the method according to claim 5, wherein the authorized users and/or the authorized processes are specified individually or as groups (fig. 3, #50).

Regarding claim 9. The method according to claim 4, wherein the conditional logic further controls access to the document component (col. 7, lines 51-57).

Regarding claim 10, Yamada discloses the method according to claim 9, wherein the key distribution information further controls access to the conditional logic (fig. 2, #41).

Regarding claim 11, Yamada discloses the method according to claim 4, wherein the document component and the conditional logic are encrypted before encapsulation

within the security container (fig. 2, #40 & 41).

Regarding claim 12, Yamada discloses the method according to claim 4, wherein the security container is encoded in structured document format (col. 7, lines 32-36).

Regarding claim 13, Yamada discloses the method according to claim 12, wherein the structured document format is Extensible Markup Language ("XML") format (col. 7, lines 32-36).

Regarding claim 14, Yamada discloses the method according to claim 5, wherein the identification of the one or more users and/or processes comprises an identification of at least one group, the group having as members one or more of the users and/or processes (fig. 13, #ST38).

Regarding claim 15, Yamada discloses the method according to claim 14, wherein the members are determined dynamically, upon receiving a request to access to the document component (fig. 13, #ST38).

Regarding claim 16, Yamada discloses the method according to claim 15, wherein the dynamic determination further comprises accessing a repository where the members of the group are identified (fig. 13, #ST38, and EEPROM, fig. 6, #23).

Regarding claim 17, Yamada discloses the method according to claim 4, further comprising the steps of: receiving, from a requester, a request to access the document component (fig. 13, #ST32); programmatically determining, using the key distribution information, whether the requester is authorized to access the document component (fig. 13, #ST43); and programmatically evaluating, using the conditional logic whether the request can be granted (fig. 13, #ST44), when the programmatically determining step has a positive result (fig 13, #ST45), and rejecting the request when the programmatically determining step has a negative result (fig. 13, #ST40).

Regarding claim 18, Yamada discloses the method according to claim 17, wherein the conditional logic evaluates at least one of: an identity of the requester; a device used by the requester; a context of the requester; a zone of an application used by the requester; a user profile of the requester; and a target destination of the request (fig. 13, #ST35-ST38).

Regarding claim 19, Yamada discloses a computer program product for securing document content using security containers, the computer program product embodied on one or more computer-readable media and comprising: computer-readable program code means for receiving, from a requester, a request to access document content (fig. 13, #S32), wherein the document content/encrypted information (fig. 2, #40) is encapsulated as a document component within a security container/recording unit (fig. 2, #29) along with conditional logic/control information (fig. 2, #42) for controlling

operations on the document component and key distribution information/encrypted key information (fig. 2, #29) usable for controlling access to the document component (col. 7, lines 51-57); computer-readable program code means for programmatically determining, using the key distribution information, whether the requester is authorized to access the document component (fig. 13, #ST38); and computer-readable program code means for programmatically evaluating, using the conditional logic, whether the request can be granted, when operation of the computer-readable program code means for programmatically determining yields a positive result (fig. 13, #ST45), and for rejecting the request when operation of the computer-readable program code means for programmatically determining yields a negative result (fig. 13, #ST40).

Regarding claim 20, Yamada discloses a system for securing document content using security containers, comprising: a security container (fig. 2, #29) that encapsulates a document component/encrypted information (fig. 2, #40 and fig. 10), conditional logic/control information (fig. 2, #42) for controlling operations on the document component, and key distribution information/encrypted key information (fig. 2, #41) usable for controlling access to the document component (col. 7, lines 51-57); means for receiving, from a requester, a request to access the document component (fig. 13, #ST32); means for programmatically determining, using the key distribution information, whether the requester is authorized to access the document component (fig. 13, #ST38); and means for programmatically evaluating, using the conditional logic, whether the request can be granted, when operation of the means for programmatically

determining yields a positive result (fig. 13, #ST44-ST45), and for rejecting the request when operation of the means for programmatically determining yields a negative result (fig. 13, #ST40).

Regarding claim 21, Yamada discloses the system according to claim 20, wherein the security container is embedded within a document (fig. 10).

Regarding claim 22, Yamada discloses the system according to claim 20, wherein the security container encapsulates the document component on a system clipboard (fig. 1, #29).

Regarding claim 23, Yamada discloses the system according to claim 20, wherein the security container is placed on a user interface (fig. 6, #29).

Regarding claim 24, Yamada discloses the system according to claim 20, wherein the security container encapsulates the document component for exchange using interprocess communications (col. 10, lines 3-21).

Regarding claim 25, Yamada discloses the system according to claim 20, wherein the security container encapsulates the document component for exchange using a messaging system (fig. 18).

Regarding claim 26, Yamada discloses the system according to claim 20, further comprising means for copying the document component to a target destination, wherein the means for copying copies the entire security container in order to copy the document component (fig. 14, #ST56).

Regarding claim 27, Yamada discloses a method of securing document content using security containers, comprising steps of: receiving, from a requester, a request to access document content (fig. 13, #ST32), wherein the document content is encapsulated as a document component/encrypted content (fig. 2, #40) within a security container (fig. 2, #29) along with conditional logic for controlling operations on the document component (fig. 2, #42) and key distribution information usable for controlling access to the document component (fig. 2, #41); programmatically determining, using the key distribution information, whether the requester is authorized to access the document component; programmatically evaluating, using the conditional logic, whether the request can be granted, when the programmatically determining step has a positive result (fig. 13, #ST45), and for rejecting the request when the programmatically determining step has a negative result (fig. 13, #ST40); and charging a fee for carrying out one of more of the receiving, programmatically determining, and programmatically evaluating steps (col. 14, lines 26-29).

Regarding claim 28, Yamada discloses a method of securing document content using security containers, comprising steps of: receiving, from a requester, a request to

access document content (fig. 13, #ST32), wherein the document content is encapsulated as a document component/encrypted content (fig. 2, #40) within a security container (fig. 2, #29) along with conditional logic for controlling operations on the document component (fig. 2, #42) and key distribution information usable for controlling access to the document component (fig. 2, #41); programmatically determining, using the key distribution information, whether the requester is authorized to access the document component; programmatically evaluating, using the conditional logic, whether the request can be granted, when the programmatically determining step has a positive result (fig. 13, #ST45), and for rejecting the request when the programmatically determining step has a negative result (fig. 13, #ST40); and charging a fee for carrying out one of more of the receiving, programmatically determining, and programmatically evaluating steps (col. 14, lines 26-29).

Regarding claim 29, Yamada discloses the method according to Claim 5, further comprising the steps of: sending the security container to one or more recipients (fig. 13, #ST43); and upon receipt at each of the recipients, using the conditional logic to determine whether that recipient can access the document component encapsulated within the security container (fig. 13, #ST44).

Regarding claim 30, Yamada discloses the method according to Claim 5, further comprising the steps of: receiving, at a recipient, the security container; and using the

conditional logic to determine whether the recipient can access the document component encapsulated within the security container (fig. 13, #ST44).

Regarding claim 31, Yamada discloses the method according to Claim 5, further comprising the steps of: receiving, at a plurality of recipients, the security container; and using the conditional logic, at one or more of the recipients, to determine whether that recipient can access the document component encapsulated within the security container (fig. 13, #ST44).

Regarding claim 32, Yamada discloses the method according to Claim 4, wherein the security container encapsulates the document component for transfer to a plurality of members of a group, and wherein each member of the group to which the transfer is made uses the conditional logic for determining whether that member is authorized to access the document component (fig. 13, #ST44).

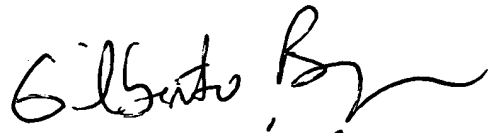
Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aubrey H. Wyszynski whose telephone number is (571)272-8155. The examiner can normally be reached on Monday - Thursday, and alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571)272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AHW



GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100